**МИНОБРНАУКИ РОССИИ**
федеральное государственное бюджетное образовательное учреждение
высшего образования
**«Самарский государственный технический университет»**
(ФГБОУ ВО «СамГТУ»)

УТВЕРЖДАЮ:
Директор филиала ФГБОУ ВО "СамГТУ" в г. Новокуйбышевске
_____ / Г.И. Заболотни
"_____" _____ 20___ г.

# РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

## ФТД.В.01 «Основы информационной безопасности»

| | |
|---|---|
| **Код и направление подготовки (специальность)** | 13.03.02 Электроэнергетика и электротехника |
| **Направленность (профиль)** | Электроэнергетика |
| **Квалификация** | Бакалавр |
| **Форма обучения** | Очная |
| **Год начала подготовки** | 2026 |
| **Институт / факультет** | Кафедры филиала ФГБОУ ВО "СамГТУ" в г. Новокуйбышевске |
| **Выпускающая кафедра** | кафедра "Электроэнергетика, электротехника и автоматизация технологических процессов" (НФ- ЭЭиАТП) |
| **Кафедра-разработчик** | кафедра "Электроэнергетика, электротехника и автоматизация технологических процессов" (НФ- ЭЭиАТП) |
| **Объем дисциплины, ч. / з.е.** | 36 / 1 |
| **Форма контроля (промежуточная аттестация)** | Зачет |

Самара 2026

**ФТД.В.01 «Основы информационной безопасности»**

Рабочая программа дисциплины разработана в соответствии с требованиями ФГОС ВО по направлению подготовки (специальности) **13.03.02 Электроэнергетика и электротехника**, утвержденного приказом Министерства образования и науки РФ от № 144 от 28.02.2018 и соответствующего учебного плана.

Разработчик РПД:

| | |
|---|---|
| Доцент, кандидат технических наук | А.А Складчиков |
| (должность, степень, ученое звание) | (ФИО) |

| | |
|---|---|
| Заведующий кафедрой | А.А. Складчиков, кандидат технических наук |
| | (ФИО, степень, ученое звание) |

СОГЛАСОВАНО:

| | |
|---|---|
| Председатель методического совета факультета / института (или учебно-методической комиссии) | Е.Т Демидова, кандидат юридических наук, доцент |
| | (ФИО, степень, ученое звание) |
| Руководитель образовательной программы | А.А. Складчиков, кандидат технических наук |
| | (ФИО, степень, ученое звание) |

Содержание

## 1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

| Наименование категории (группы) компетенций | Код и наименование компетенции | Код и наименование индикатора достижения компетенции | Результаты обучения (знать, уметь, владеть, соотнесенные с индикаторами достижения компетенции) |
|---|---|---|---|
| Универсальные компетенции | | | |
| Безопасность жизнедеятельности | УК-8 Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов | УК-8.2 Понимает, как создавать и поддерживать безопасные условия жизнедеятельности, том числе при возникновении чрезвычайных ситуаций и военных конфликтов. | Владеть навыками использования методов организации и контроля функционирования системы защиты информации навыками использования стандартов для защиты информации в информационной системе |
| | | | Знать основные законодательные и нормативные документы федерального уровня в области информационной безопасности и защиты информации содержание основных уровней обеспечения информационной безопасности |
| | | | Уметь выполнять анализ требований к системе защиты информации выявлять угрозы информационной безопасности, обосновывать организационно-технические мероприятия по защите информации в информационной системе |

## 2. Место дисциплины (модуля) в структуре образовательной программы

Место дисциплины (модуля) в структуре образовательной программы: **блок факультативных дисциплин**

| Код компетенции | Предшествующие дисциплины | Параллельно осваиваемые дисциплины | Последующие дисциплины |
|---|---|---|---|
| УК-8 | | Безопасность жизнедеятельности; Основы военной подготовки | Государственная итоговая аттестация: подготовка к процедуре защиты и защита выпускной квалификационной работы; Экология |

## 3. Объем дисциплины (модуля) в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

| Вид учебной работы | Всего часов / часов в электронной форме | 4 семестр часов / часов в электронной форме |
|---|---|---|
| **Аудиторная контактная работа (всего),** в том числе: | 16 | 16 |
| Лекции | 4 | 4 |
| Практические занятия | 12 | 12 |
| **Самостоятельная работа (всего),** в том числе: | 20 | 20 |
| выполнение задач, заданий, упражнений (в том числе разноуровневых) | 10 | 10 |
| подготовка к зачету | 10 | 10 |
| **Итого: час** | 36 | 36 |
| **Итого: з.е.** | 1 | 1 |

## 4. Содержание дисциплины (модуля), структурированное по темам (разделам), с указанием отведенного на них количества академических часов и видов учебных занятий

| № раздела | Наименование раздела дисциплины | Виды учебной нагрузки и их трудоемкость, часы | | | | |
|---|---|---|---|---|---|---|
| | | ЛЗ | ЛР | ПЗ | СРС | Всего часов |
| 1 | Основы информационной безопасности | 4 | 0 | 12 | 20 | 36 |
| | **Итого** | 4 | 0 | 12 | 20 | 36 |

### 4.1 Содержание лекционных занятий

| № занятия | Наименование раздела | Тема лекции | Содержание лекции (перечень дидактических единиц: рассматриваемых подтем, вопросов) | Количество часов / часов в электронной форме |
|---|---|---|---|---|
| **4 семестр** | | | | |
| 1 | Основы информационной безопасности | Изучение методики управления рисками для анализа рисков личной информационной безопасности | Изучить методику для систематизации и анализа рисков по приведенным в приложении материалам курса С.А.Нестерова и "Руководства по управлению рисками". На основании собранных на лабораторном занятии №1 данных о неприкосновенность частной жизни идентифицировать риски личной информационной безопасности и создать их полное описание по определению методики. Выполнить этап "Поддержка принятия решений". Разработать план мероприятий по осуществлению этапов "Реализация контроля" и "Оценка эффективности программы". | 2 |
| 2 | Основы информационной безопасности | Изучение методов оценивания воздействия ИКТ-технологий на неприкосновенность частной жизни. | Воспитание ответственного отношения к информационной деятельности, связанной с обработкой и хранением информации; Приобретение опыта профилактической и предупреждающей деятельности по отношению к информационным угрозам на уровне личной информационной безопасности | 2 |
| | | | **Итого за семестр:** | **4** |
| | | | **Итого:** | **4** |

## 4.2 Содержание лабораторных занятий

Учебные занятия не реализуются.

## 4.3 Содержание практических занятий

| № занятия | Наименование раздела | Тема практического занятия | Содержание практического занятия (перечень дидактических единиц: рассматриваемых подтем, вопросов) | Количество часов / часов в электронной форме |
|---|---|---|---|---|
| **4 семестр** | | | | |
| 1 | Основы информационной безопасности | Аутентификация, разрешениями на файлы и папки Управление | Управления разрешениями на файлы и папки Windows. Управление доступом к файлам. | 2 |

| | | | | |
|---|---|---|---|---|
| 2 | Основы информационной безопасности | Применение методики управления рисками для анализа рисков личной информационной безопасности | Изучить методику для систематизации и анализа рисков по приведенным в приложении материалам курса С.А.Нестерова и "Руководства по управлению рисками". На основании собранных на лабораторном занятии №1 данных о неприкосновенность частной жизни идентифицировать риски личной информационной безопасности и создать их полное описание по определению методики. Выполнить этап "Поддержка принятия решений". Разработать план мероприятий по осуществлению этапов "Реализация контроля" и "Оценка эффективности программы". | 2 |
| 3 | Основы информационной безопасности | Анализ безопасности протокола обмена информацией | Найти уязвимость в схеме протокола. Определить, атака какого типа позволит воспользоваться выявленной уязвимостью протокола. Предложить способ модифицировать протокол, чтобы устранить уязвимость. | 2 |
| 4 | Основы информационной безопасности | Обзор функций безопасности Windows | Приобрести практические навыки использования технологий BitLocker, IPSec, MMC, UAC, встроенных в Windows. | 2 |
| 5 | Основы информационной безопасности | Разработка политики информационной безопасности | Разработать политику информационной безопасности подразделения с использованием общепринятых шаблонов и учетом специфики деятельности организации. | 2 |
| 6 | Основы информационной безопасности | Настройка Интернет-браузера для безопасной работы | Изучение настроек безопасности для различных браузеров. | 2 |
| | | | **Итого за семестр:** | **12** |
| | | | **Итого:** | **12** |

## 4.4. Содержание самостоятельной работы

| **Наименование раздела** | **Вид самостоятельной работы** | **Содержание самостоятельной работы** (перечень дидактических единиц: рассматриваемых подтем, вопросов) | **Количество часов** |
|---|---|---|---|
| **4 семестр** | | | |
| Основы информационной безопасности | Повторение всех тем входящих в дисциплину. | Повторение всех тем входящих в дисциплину. | 20 |
| | | **Итого за семестр:** | **20** |
| | | **Итого:** | **20** |

## 5. Перечень учебной литературы и учебно-методического обеспечения по

**дисциплине (модулю)**

| № п/п | Библиографическое описание | Ресурс НТБ СамГТУ (ЭБС СамГТУ, IPRbooks и т.д.) |
|---|---|---|
| Основная литература | | |
| 1 | Лазарев, Ю.Н. Программно-технические методы защиты информации : учеб.-мтод.пособие / Ю. Н. Лазарев, Ф. Ф. Буканов; Самар.гос.техн.ун-т, Электронные системы и информационная безопасность.- Самара, 2007.- 94 с..- Режим доступа: https://elib.samgtu.ru/getinfo?uid=els_samgtu\|\|elib\|\|721 | Электронный ресурс |
| Дополнительная литература | | |
| 2 | Беляева, Г.И. Информационная безопасность : лабораторный практикум / Г. И. Беляева; Самарский государственный технический университет, Национальная и мировая экономика.- Самара, 2024.- 41 с..- Режим доступа: https://elib.samgtu.ru/getinfo?uid=els_samgtu\|\|elib\|\|6239 | Электронный ресурс |
| 3 | Ворожейкин, В.Н. Технические средства и методы защиты информации – дополнительные главы : Лабораторный практикум / В. Н. Ворожейкин; Самар.гос.техн.ун-т, Электронные системы и информационная безопасность .- 2-е изд..- Самара, 2019.- 336 с..- Режим доступа: https://elib.samgtu.ru/getinfo?uid=els_samgtu\|\|elib\|\|3574 | Электронный ресурс |
| Учебно-методическое обеспечение | | |
| 4 | Овсянников, А.С. Теория информационных процессов и систем. Ч. 1 Теоретические основы информационных процессов : учебное пособие / А. С. Овсянников; Самарский государственный технический университет, Самарский государственный архитектурно-строительный университет, Прикладная математика и вычислительная техника.- Самара, 2001.- 84 с..- Режим доступа: https://elib.samgtu.ru/getinfo?uid=els_samgtu\|\|elib\|\|4745 | Электронный ресурс |

Доступ обучающихся к ЭР НТБ СамГТУ (elib.samgtu.ru) осуществляется посредством электронной информационной образовательной среды университета и сайта НТБ СамГТУ по логину и паролю.

## 6. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения

При проведении лекционных занятий используется мультимедийное оборудование.

Организовано взаимодействие обучающегося и преподавателя с использованием электронной ин-формационной образовательной среды университета.

| № п/п | Наименование | Производитель | Способ распространения |
|---|---|---|---|
| 1 | Microsoft Office | Microsoft (Зарубежный) | Лицензионное |

## 7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», профессиональных баз данных, информационно-справочных систем

| № п/п | Наименование | Краткое описание | Режим доступа |
|---|---|---|---|
| 1 | Электронно-библиотечная система IPRbooks | http://www.iprbookshop.ru/ | Российские базы данных ограниченного доступа |

## 8. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)

**Лекционные занятия**

Аудитория для лекционных, семинарских и практических занятий, текущего контроля и промежуточной аттестации (с мультимедийным оборудованием) укомплектованы мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории.

**Практические занятия**

Аудитория для практических и семинарских занятий, текущего контроля и промежуточной аттестации, укомплектованные специализированной мебелью и техническими средствами обучения (проектор, экран, компьютер/ноутбук), с выходом в сеть Интернет и доступом в электронную информационно-образовательную среду СамГТУ. Аудитория оборудована специализированной мебелью: столы и стулья для обучающихся; стол и стул для преподавателя, доска.

- компьютерные классы (ауд. 101, 102, 111, 201, 311,401, 404).

**Самостоятельная работа**

Помещения для самостоятельной работы оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и доступом к электронной информационно-образовательной среде СамГТУ:

- Кабинет для текущего контроля и промежуточной аттестации, курсового проектирования, групповых и индивидуальных консультаций ауд. 212;
- Кабинет для самостоятельной работы, аудитория 304;
- компьютерные классы (ауд. 101, 102, 111, 201, 311,401, 404).

## 9. Методические материалы

### Методические рекомендации при работе на лекции

До лекции студент должен просмотреть учебно-методическую и научную литературу по теме лекции с тем, чтобы иметь представление о проблемах, которые будут разбираться в лекции.

Перед началом лекции обучающимся сообщается тема лекции, план, вопросы, подлежащие рассмотрению, доводятся основные литературные источники. Весь учебный материал, сообщаемый преподавателем, должен не просто прослушиваться. Он должен быть активно воспринят, т.е. услышан, осмыслен, понят, зафиксирован на бумаге и закреплен в памяти. Приступая к слушанию нового учебного материала, полезно мысленно установить его связь с ранее изученным. Следя за техникой чтения лекции (акцент на существенном, повышение тона, изменение ритма, пауза и т.п.), необходимо вслед за преподавателем уметь выделять основные категории, законы и определять их содержание, проблемы, предполагать их возможные решения, доказательства и выводы. Осуществляя такую работу, можно значительно облегчить себе понимание учебного материала, его конспектирование и дальнейшее изучение.

Конспектирование лекции позволяет обработать, систематизировать и лучше сохранить полученную информацию с тем, чтобы в будущем можно было восстановить в памяти основные, содержательные моменты. Типичная ошибка, совершаемая обучающимся, дословное конспектирование речи преподавателя. Как правило, при записи «слово в слово» не остается времени на обдумывание, анализ и синтез информации. Отбирая нужную информацию, главные мысли, проблемы, решения и выводы, необходимо сокращать текст, строить его таким образом, чтобы потом можно было легко в нем разобраться. Желательно оставить в рабочих конспектах поля, на которых можно будет делать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений. С окончанием лекции работа над конспектом не может считаться завершенной. Нужно еще восстановить отдельные места, проверить, все ли понятно, уточнить что-то на консультации и т.п. с тем, чтобы конспект мог быть использован в процессе подготовки к практическим занятиям, зачету, экзамену. Конспект лекции – незаменимый учебный документ, необходимый для самостоятельной работы.

## Методические рекомендации при подготовке и работе на практическом занятии

Практические занятия по дисциплине проводятся в целях выработки практических умений и приобретения навыков в решении профессиональных задач.

Рекомендуется следующая схема подготовки к практическому занятию:

1. ознакомление с планом практического занятия, который отражает содержание предложенной темы;
2. проработка конспекта лекции;
3. чтение рекомендованной литературы;
4. подготовка ответов на вопросы плана практического занятия;
5. выполнение тестовых заданий, задач и др.

Подготовка обучающегося к практическому занятию производится по вопросам, разработанным для каждой темы практических занятий и (или) лекций. В процессе подготовки к практическим занятиям, необходимо обратить особое внимание на самостоятельное изучение рекомендованной литературы.

Работа студентов во время практического занятия осуществляется на основе заданий, которые выдаются обучающимся в начале или во время занятия. На практических занятиях приветствуется активное участие в обсуждении конкретных ситуаций, способность на основе полученных знаний находить наиболее эффективные решения поставленных проблем, уметь находить полезный дополнительный материал по тематике занятий. Обучающимся необходимо обращать внимание на основные понятия, алгоритмы, определять практическую значимость рассматриваемых вопросов. На практических занятиях обучающиеся должны уметь выполнить расчет по заданным параметрам или выработать определенные решения по обозначенной проблеме. Задания могут быть групповые и индивидуальные. В зависимости от сложности предлагаемых заданий, целей занятия, общей подготовки обучающихся преподаватель может подсказать обучающимся алгоритм решения или первое действие, или указать общее направление рассуждений. Полученные результаты обсуждаются с позиций их адекватности или эффективности в рассмотренной ситуации.

## Методические рекомендации по выполнению самостоятельной работы

Организация самостоятельной работы обучающихся ориентируется на активные методы

овладения знаниями, развитие творческих способностей, переход от поточного к индивидуализированному обучению с учетом потребностей и возможностей обучающегося.

Самостоятельная работа с учебниками, учебными пособиями, научной, справочной литературой, материалами периодических изданий и Интернета является наиболее эффективным методом получения дополнительных знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала. Все новые понятия по изучаемой теме необходимо выучить наизусть и внести в глоссарий, который целесообразно вести с самого начала изучения курса.

Самостоятельная работа реализуется:

- непосредственно в процессе аудиторных занятий;
- на лекциях, практических занятиях;
- в контакте с преподавателем вне рамок расписания;
- на консультациях по учебным вопросам, в ходе творческих контактов, при ликвидации задолженностей, при выполнении индивидуальных заданий и т.д.;
- в библиотеке, дома, на кафедре при выполнении обучающимся учебных и практических задач.

Эффективным средством осуществления обучающимся самостоятельной работы является электронная информационно-образовательная среда университета, которая обеспечивает доступ к учебным планам, рабочим программам дисциплин (модулей), практик, к изданиям электронных библиотечных систем.

## 10. Фонд оценочных средств по дисциплине (модулю)

Фонд оценочных средств представлен в приложении № 1.

Приложение 1 к рабочей программе дисциплины
ФТД.В.01 «Основы информационной безопасности»

**Фонд оценочных средств**
**по дисциплине**
**ФТД.В.01 «Основы информационной безопасности»**

| | |
|---|---|
| **Код и направление подготовки (специальность)** | 13.03.02 Электроэнергетика и электротехника |
| **Направленность (профиль)** | Электроэнергетика |
| **Квалификация** | Бакалавр |
| **Форма обучения** | Очная |
| **Год начала подготовки** | 2026 |
| **Институт / факультет** | Кафедры филиала ФГБОУ ВО "СамГТУ" в г. Новокуйбышевске |
| **Выпускающая кафедра** | кафедра "Электроэнергетика, электротехника и автоматизация технологических процессов" (НФ- ЭЭиАТП) |
| **Кафедра-разработчик** | кафедра "Электроэнергетика, электротехника и автоматизация технологических процессов" (НФ- ЭЭиАТП) |
| **Объем дисциплины, ч. / з.е.** | 36 / 1 |
| **Форма контроля (промежуточная аттестация)** | Зачет |

## Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

| Наименование категории (группы) компетенций | Код и наименование компетенции | Код и наименование индикатора достижения компетенции | Результаты обучения (знать, уметь, владеть, соотнесенные с индикаторами достижения компетенции) |
|---|---|---|---|
| Универсальные компетенции | | | |
| Безопасность жизнедеятельности | УК-8 Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов | УК-8.2 Понимает, как создавать и поддерживать безопасные условия жизнедеятельности, том числе при возникновении чрезвычайных ситуаций и военных конфликтов. | Владеть навыками использования методов организации и контроля функционирования системы защиты информации навыками использования стандартов для защиты информации в информационной системе |
| | | | Знать основные законодательные и нормативные документы федерального уровня в области информационной безопасности и защиты информации содержание основных уровней обеспечения информационной безопасности |
| | | | Уметь выполнять анализ требований к системе защиты информации выявлять угрозы информационной безопасности, обосновывать организационно-технические мероприятия по защите информации в информационной системе |

## Матрица соответствия оценочных средств запланированным результатам обучения

| Код индикатора достижения компетенции | Результаты обучения | Оценочные средства | Текущий контроль успеваемости | Промежуточная аттестация |
|---|---|---|---|---|
| **Основы информационной безопасности** | | | | |
| УК-8.2 Понимает, как создавать и поддерживать безопасные условия жизнедеятельности, том числе при возникновении чрезвычайных ситуаций и военных конфликтов. | **Уметь** выполнять анализ требований к системе защиты информации выявлять угрозы информационной безопасности, обосновывать организационно-технические мероприятия по защите информации в информационной системе | вопросы промежуточной аттестации | Да | Да |
| | **Владеть** навыками использования методов организации и контроля функционирования системы защиты информации навыками использования стандартов для защиты информации в информационной системе | вопросы промежуточной аттестации | Да | Да |
| | **Знать** основные законодательные и нормативные документы федерального уровня в области информационной безопасности и защиты информации содержание основных уровней обеспечения информационной безопасности | вопросы промежуточной аттестации | Да | Да |

***Типовые задания для промежуточной аттестации по дисциплине***
***ФТД.В.01 «Основы информационной безопасности»***
*(шифр и наименование дисциплины)*

***для направления подготовки 13.03.02 Электроэнергетика и электротехника***
*(шифр и наименование направления подготовки, специальности)*

**2025 ГОД ПРИЕМА**
*(год приема на образовательную программу)*

***Контролируемая (ые) компетенция(и):***
***УК-8 Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов***
*(шифр и наименование компетенции(й))*

**Количество заданий в комплекте оценочных материалов**

| Код компетенции | Наименование компетенции | Количество заданий |
|---|---|---|
| УК-8 | Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов | 60 |

**Сценарии выполнения диагностических заданий**

| Тип задания | Последовательность действий при выполнении задания |
|---|---|
| Задание закрытого типа с однозначным выбором варианта ответа | 1. Внимательно прочитать текст задания.<br>2. Выбрать единственный вариант ответа из предложенных. |
| Задание закрытого типа с многозначным выбором вариантов ответа | 1. Внимательно прочитать текст задания.<br>2. Выбрать несколько вариантов ответа из предложенных. |
| Задание закрытого типа на установление соответствия | 1. Внимательно прочитать текст задания и понять, что<br>в качестве ответа ожидаются пары элементов.<br>2. Внимательно прочитать оба списка: список 1 - вопросы, утверждения, факты, понятия и т.д.; список 2 - утверждения, свойства объектов и т.д.<br>3. Сопоставить элементы списка 1 с элементами списка 2, сформировать пары элементов.<br>4. Записать буквы вариантов ответа (например, АБВГ) |
| Задание закрытого типа на установление последовательности | 1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается последовательность элементов.<br>2. Внимательно прочитать предложенные варианты ответа.<br>3. Построить верную последовательность из предложенных элементов.<br>4. Записать буквы вариантов ответа в нужной последовательности без пробелов и знаков препинания (например, БВА) |
| Задание открытого типа на дополнение | 1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается недостающее дополнение.<br>2. Определить какой информации не хватает.<br>3. Внесение пропущенного слова.<br>4. Записать в ответ только дополнение. |
| Задание открытого типа с развернутым ответом | 1. Внимательно прочитать текст задания и понять суть вопроса.<br>2. Продумать логику и полноту ответа.<br>3. Записать ответ, используя четкие компактные формулировки.<br>4. В случае расчетной задачи записать решение и ответ. |
| Задание комбинированного типа: практико-ориентированные задания | 1. Внимательно прочитать текст задания.<br>2. Выполните указанные в задания действия |
| Задание комбинированного типа с выбором одного ответа и обоснованием выбора ответа | 1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается только один из предложенных вариантов.<br>2. Внимательно прочитать предложенные варианты ответа.<br>3. Выбрать один ответ, наиболее верный.<br>4. Записать только букву выбранного варианта ответа.<br>5. Записать аргументы, обосновывающие выбор ответа |
| Задание комбинированного типа с выбором нескольких ответов и обоснованием выборов ответов | 1. Внимательно прочитать текст задания и понять, что в качестве ответа ожидается несколько из предложенных вариантов.<br>2. Внимательно прочитать предложенные варианты ответа.<br>3. Выбрать несколько верных вариантов ответов. |

| | |
|---|---|
| | 4. Записать последовательно буквы выбранных вариантов без пробелов и знаков препинания (например, АБВ).<br>5. Записать аргументы, обосновывающие выбор каждого из ответов |

**Система оценивания заданий**

| Указания по оцениванию | Результат оценивания (баллы, полученные за выполнение задания / характеристика правильности ответа) |
|---|---|
| Задание закрытого типа с однозначным выбором варианта ответа считается верным, если правильно определен вариант ответа | За правильный вариант ответа начисляется 1 балл |
| Задание закрытого типа с многозначным выбором вариантов ответа считается верным, если правильно определены все варианты ответа | За правильный вариант ответа начисляется 1 балл |
| Задание закрытого типа на установление соответствия считается верным, если правильно установлены все соответствия (позиции из одного столбца верно сопоставлены с позициями другого) | Количество баллов определяется числом пар для сопоставления. За каждое правильно установленное соответствие начисляется 1 балл. |
| Задание закрытого типа на установление последовательности считается верным, если правильно указана вся последовательность цифр | Максимальный балл определяется количеством элементов в последовательности. В случае ошибки в одном месте - снижение на один балл. За каждое правильно указанное место элемента в последовательности начисляется 1 балл. |
| Задание открытого типа на дополнение, где предоставляется предложение или фрагмент текста, в котором пропущено одно или несколько слов или фраз. Задача состоит в том, чтобы заполнить пропуски, восстановив тем самым исходный смысл предложения. | 2 балла засчитывается, если студент вписал правильный ответ в соответствии с ключом.<br>1 балл может быть засчитан за близкий к правильному ответ, если он демонстрирует частичное понимание. |
| Задание открытого типа с развернутым ответом считается верным, если ответ совпадает с эталонным по содержанию и полноте | Максимальный балл - 4. Студент может получить 4 балла за полный и правильный ответ, логично изложенный и с корректной терминологией, или меньше за неполные или неточно сформулированные ответы. Полнота (1 балл), Правильность (1 балл), Логичность (1 балл), Терминология (1 балл). |
| Задание комбинированного типа с выбором одного ответа и обоснованием выбора ответа считается верным, если правильно указана цифра и приведены корректные аргументы, используемые при выборе ответа | За правильный выбор ответа начисляется 1 балл. За качественное обоснование - еще 2-3 балла. Критерии оценивания обоснования должны быть четко определены (например, логичность, полнота, использование фактов). Неправильный выбор ответа - 0 баллов, даже если обоснование частично верное. |
| Задание комбинированного типа с выбором нескольких вариантов ответа и обоснованием выбора ответа считается верным, если правильно указана цифра и приведены корректные аргументы, используемые при выборе ответа | За правильный выбор ответа начисляется 1 балл. За качественное обоснование - еще 2-3 балла. Критерии оценивания обоснования должны быть четко определены (например, логичность, полнота, использование фактов). Неправильный выбор ответа - 0 баллов, даже если обоснование частично верное. |

| *№ задания* | *Содержание задания* | *Ответ на задание* | *Тип задания* | *Время выполнения задания, мин* | *Уровень сложности (балл)* | *№ Темы* |
|---|---|---|---|---|---|---|
| ПК-2 Способен применять средства и методы обеспечения информационной безопасности в пользовательских и корпоративных информационных системах | | | | | | |
| 1. | Прочитайте текст вопроса и выберите правильный ответ.<br><br>Что является основной целью аутентификации пользователя в информационной системе?<br>A) Подтверждение личности пользователя<br>B) Удаление временных файлов<br>C) Шифрование всех документов | Правильный ответ: A<br>Пояснение: Аутентификация используется для проверки, что пользователь является тем, за кого себя выдает. | Закрытый с выбором одного ответа | 1 | 1 | 1 |

| *№ задания* | *Содержание задания* | *Ответ на задание* | *Тип задания* | *Время выполнения задания, мин* | *Уровень сложности (балл)* | *№ Темы* |
|---|---|---|---|---|---|---|
| | D) Ускорение загрузки системы | | | | | |
| 2. | Прочитайте текст вопроса и выберите правильный ответ.<br><br>Какой механизм Windows применяется для разграничения доступа к файлам и папкам?<br>A) Буфер обмена<br>B) NTFS-разрешения<br>C) Диспетчер задач<br>D) Архивация данных | Правильный ответ: B<br>Пояснение: NTFS-разрешения позволяют задавать права чтения, записи и изменения для пользователей и групп. | Закрытый с выбором одного ответа | 1 | 1 | 1 |
| 3. | Прочитайте текст вопроса и выберите правильный ответ.<br><br>Что в методике управления рисками называется риском информационной безопасности?<br>A) Любое установленное приложение<br>B) Возможность реализации угрозы с негативными последствиями<br>C) Скорость работы компьютера<br>D) Количество файлов на диске | Правильный ответ: B<br>Пояснение: Риск связан с вероятностью угрозы и возможным ущербом для информации или системы. | Закрытый с выбором одного ответа | 1 | 1 | 2 |
| 4. | Прочитайте текст вопроса и выберите правильный ответ.<br><br>Какой этап обычно выполняется первым при анализе рисков личной информационной безопасности?<br>A) Выбор цвета интерфейса<br>B) Выявление защищаемых активов<br>C) Удаление операционной системы<br>D) Покупка нового монитора | Правильный ответ: B<br>Пояснение: Сначала определяют, какие данные и ресурсы необходимо защищать. | Закрытый с выбором одного ответа | 1 | 1 | 2 |
| 5. | Прочитайте текст вопроса и выберите правильный ответ.<br><br>Что является основной целью анализа безопасности протокола обмена информацией?<br>A) Оценить дизайн сайта<br>B) Найти уязвимости в передаче данных<br>C) Увеличить размер файлов<br>D) Отключить сетевое оборудование | Правильный ответ: B<br>Пояснение: Анализ протокола позволяет определить слабые места в обмене данными. | Закрытый с выбором одного ответа | 1 | 1 | 3 |
| 6. | Прочитайте текст вопроса и выберите правильный ответ. | Правильный ответ: A<br>Пояснение: BitLocker | Закрытый с | 1 | 1 | 4 |

| *№ задания* | *Содержание задания* | *Ответ на задание* | *Тип задания* | *Время выполнения задания, мин* | *Уровень сложности (балл)* | *№ Темы* |
|---|---|---|---|---|---|---|
| | Какое средство Windows предназначено для шифрования дисков?<br>A) BitLocker<br>B) Paint<br>C) WordPad<br>D) Корзина | защищает данные на диске с помощью шифрования. | выбором одного ответа | | | |
| 7. | Прочитайте текст вопроса и выберите правильный ответ.<br><br>Какое средство Windows помогает запрашивать подтверждение при выполнении административных действий?<br>A) UAC<br>B) IPSec<br>C) MMC<br>D) Проводник | Правильный ответ: A<br>Пояснение: UAC снижает риск несанкционированного изменения настроек системы. | Закрытый с выбором одного ответа | 1 | 1 | 4 |
| 8. | Прочитайте текст вопроса и выберите правильный ответ.<br><br>Что такое политика информационной безопасности организации?<br>A) Случайный список паролей<br>B) Документ с правилами защиты информации<br>C) График отпусков сотрудников<br>D) Инструкция по ремонту мебели | Правильный ответ: B<br>Пояснение: Политика ИБ определяет требования, правила и ответственность за защиту информации. | Закрытый с выбором одного ответа | 1 | 1 | 5 |
| 9. | Прочитайте текст вопроса и выберите правильный ответ.<br><br>Какой параметр браузера повышает безопасность при работе в сети Интернет?<br>A) Отключение обновлений<br>B) Блокировка опасных сайтов и всплывающих окон<br>C) Сохранение всех паролей в открытом виде<br>D) Установка неизвестных расширений | Правильный ответ: B<br>Пояснение: Защитные настройки браузера снижают вероятность перехода на вредоносные ресурсы. | Закрытый с выбором одного ответа | 1 | 1 | 6 |
| 10. | Прочитайте текст вопроса и выберите правильный ответ.<br><br>Что рекомендуется делать с расширениями браузера для безопасной работы?<br>A) Устанавливать только из надежных источников | Правильный ответ: A<br>Пояснение: Расширения могут получать доступ к данным пользователя, поэтому важна проверка источника. | Закрытый с выбором одного ответа | 1 | 1 | 6 |

| *№ задания* | *Содержание задания* | *Ответ на задание* | *Тип задания* | *Время выполнения задания, мин* | *Уровень сложности (балл)* | *№ Темы* |
|---|---|---|---|---|---|---|
| | B) Устанавливать все предлагаемые расширения<br>C) Отключать антивирус перед установкой<br>D) Передавать им все пароли | | | | | |
| 11. | Прочитайте текст вопроса и выберите правильные ответы.<br><br>Какие элементы могут использоваться для аутентификации пользователя?<br>A) Пароль<br>B) Биометрический признак<br>C) Одноразовый код<br>D) Размер экрана<br>E) Название папки | Правильный ответ: A, B, C<br>Пояснение: Пароль, биометрия и одноразовый код подтверждают личность пользователя. | Закрытый с выбором нескольких ответов | 1 | 1 | 1 |
| 12. | Прочитайте текст вопроса и выберите правильные ответы.<br><br>Какие права доступа к файлам и папкам относятся к типовым разрешениям Windows?<br>A) Чтение<br>B) Запись<br>C) Изменение<br>D) Смена обоев рабочего стола<br>E) Полный доступ | Правильный ответ: A, B, C, E<br>Пояснение: NTFS-разрешения включают чтение, запись, изменение и полный доступ. | Закрытый с выбором нескольких ответов | 1 | 1 | 1 |
| 13. | Прочитайте текст вопроса и выберите правильные ответы.<br><br>Какие действия относятся к управлению рисками личной информационной безопасности?<br>A) Идентификация угроз<br>B) Оценка вероятности и ущерба<br>C) Выбор мер защиты<br>D) Увеличение яркости экрана<br>E) Контроль эффективности мер | Правильный ответ: A, B, C, E<br>Пояснение: Управление рисками включает выявление, оценку, обработку и контроль рисков. | Закрытый с выбором нескольких ответов | 1 | 1 | 2 |
| 14. | Прочитайте текст вопроса и выберите правильные ответы.<br><br>Какие данные можно отнести к личным информационным активам?<br>A) Паспортные данные<br>B) Пароли<br>C) Фотографии и документы<br>D) Список системных шрифтов<br>E) Данные банковских карт | Правильный ответ: A, B, C, E<br>Пояснение: Личные активы включают данные, утечка которых может причинить ущерб пользователю. | Закрытый с выбором нескольких ответов | 1 | 1 | 2 |
| 15. | Прочитайте текст вопроса и | Правильный ответ: A, B, C | Закрыт | 1 | 1 | 3 |

| *№ задания* | *Содержание задания* | *Ответ на задание* | *Тип задания* | *Время выполнения задания, мин* | *Уровень сложности (балл)* | *№ Темы* |
|---|---|---|---|---|---|---|
| | выберите правильные ответы.<br><br>Какие признаки могут указывать на уязвимость протокола обмена информацией?<br>A) Передача пароля в открытом виде<br>B) Отсутствие проверки целостности<br>C) Отсутствие аутентификации сторон<br>D) Использование документации<br>E) Шифрование канала | Пояснение: Открытая передача секретов и отсутствие контроля целостности или аутентификации создают уязвимости. | ый с выбором нескольких ответов | | | |
| 16. | Прочитайте текст вопроса и выберите правильные ответы.<br><br>Какие технологии относятся к функциям безопасности Windows?<br>A) BitLocker<br>B) UAC<br>C) IPSec<br>D) MMC<br>E) Калькулятор | Правильный ответ: A, B, C, D<br>Пояснение: BitLocker, UAC, IPSec и MMC применяются для защиты, администрирования и настройки безопасности. | Закрытый с выбором нескольких ответов | 1 | 1 | 4 |
| 17. | Прочитайте текст вопроса и выберите правильные ответы.<br><br>Какие задачи может решать BitLocker?<br>A) Шифрование системного диска<br>B) Защита данных при потере устройства<br>C) Запрос ключа восстановления<br>D) Автоматическое написание отчетов<br>E) Удаление вирусов без антивируса | Правильный ответ: A, B, C<br>Пояснение: BitLocker предназначен для защиты данных на накопителе, а не для удаления вредоносных программ. | Закрытый с выбором нескольких ответов | 1 | 1 | 4 |
| 18. | Прочитайте текст вопроса и выберите правильные ответы.<br><br>Какие разделы целесообразно включать в политику информационной безопасности?<br>A) Цели и область действия<br>B) Права и обязанности пользователей<br>C) Правила управления доступом<br>D) Любимые сайты сотрудников<br>E) Ответственность за нарушения | Правильный ответ: A, B, C, E<br>Пояснение: Политика ИБ должна закреплять требования, роли и ответственность. | Закрытый с выбором нескольких ответов | 1 | 1 | 5 |
| 19. | Прочитайте текст вопроса и выберите правильные ответы. | Правильный ответ: A, B, C, E<br>Пояснение: Обновления, проверка адреса, | Закрытый с выбор | 1 | 1 | 6 |

| *№ задания* | *Содержание задания* | *Ответ на задание* | *Тип задания* | *Время выполнения задания, мин* | *Уровень сложности (балл)* | *№ Темы* |
|---|---|---|---|---|---|---|
| | Какие действия повышают безопасность работы в браузере?<br>A) Регулярное обновление браузера<br>B) Проверка адреса сайта<br>C) Запрет сохранения паролей на чужом компьютере<br>D) Установка неизвестных расширений<br>E) Использование HTTPS-соединений | осторожность с паролями и HTTPS снижают риски. | ом нескольких ответов | | | |
| 20. | Прочитайте текст вопроса и выберите правильные ответы.<br><br>Какие угрозы связаны с небезопасной настройкой браузера?<br>A) Фишинг<br>B) Кража сохраненных паролей<br>C) Установка вредоносных расширений<br>D) Повышение разрешения экрана<br>E) Перехват данных на небезопасных сайтах | Правильный ответ: A, B, C, E<br>Пояснение: Небезопасные настройки браузера повышают риск фишинга, утечек и установки вредоносных компонентов. | Закрытый с выбором нескольких ответов | 1 | 1 | 6 |
| 21. | Установите правильное соответствие между списком 1 и списком 2. Запишите буквы и соответствующие им цифры. Пример: A-II, B-I, C-IV, D-III<br><br>Установите соответствие между понятием и его назначением.<br>Список 1:<br>A) Аутентификация<br>B) Авторизация<br>C) Учетная запись<br>D) Разрешение NTFS<br>Список 2:<br>I. Определяет допустимые действия с объектом<br>II. Проверяет личность пользователя<br>III. Предоставляет права после проверки личности<br>IV. Хранит сведения о пользователе | Правильный ответ: A-II, B-III, C-IV, D-I<br>Пояснение: Соответствия отражают назначение понятий и средств защиты. | Закрытый на сопоставление | 3 | 2 | 1 |
| 22. | Установите правильное соответствие между списком 1 и списком 2. Запишите буквы и соответствующие им цифры. Пример: A-II, B-I, C-IV, D-III | Правильный ответ: A-I, B-II, C-III, D-IV<br>Пояснение: Соответствия отражают назначение понятий и средств защиты. | Закрытый на сопоставление | 3 | 2 | 1 |

| *№ задания* | *Содержание задания* | *Ответ на задание* | *Тип задания* | *Время выполнения задания, мин* | *Уровень сложности (балл)* | *№ Темы* |
|---|---|---|---|---|---|---|
| | Установите соответствие между правом доступа и его смыслом.<br>Список 1:<br>A) Чтение<br>B) Запись<br>C) Изменение<br>D) Полный доступ<br>Список 2:<br>I. Просмотр содержимого файла или папки<br>II. Создание и изменение данных<br>III. Изменение и удаление объектов<br>IV. Все действия, включая изменение разрешений | | | | | |
| 23. | Установите правильное соответствие между списком 1 и списком 2. Запишите буквы и соответствующие им цифры.<br>Пример: A-II, B-I, C-IV, D-III<br><br>Установите соответствие между этапом анализа риска и его содержанием.<br>Список 1:<br>A) Идентификация актива<br>B) Выявление угрозы<br>C) Оценка риска<br>D) Выбор меры защиты<br>Список 2:<br>I. Определение ценной информации<br>II. Определение возможного источника ущерба<br>III. Сравнение вероятности и последствий<br>IV. Подбор способа снижения риска | Правильный ответ: A-I, B-II, C-III, D-IV<br>Пояснение: Соответствия отражают назначение понятий и средств защиты. | Закрытый на сопоставление | 3 | 2 | 2 |
| 24. | Установите правильное соответствие между списком 1 и списком 2. Запишите буквы и соответствующие им цифры.<br>Пример: A-II, B-I, C-IV, D-III<br><br>Установите соответствие между личным активом и примером угрозы.<br>Список 1:<br>A) Пароль<br>B) Смартфон<br>C) Документы<br>D) Почтовый ящик<br>Список 2:<br>I. Кража или потеря устройства | Правильный ответ: A-II, B-I, C-IV, D-III<br>Пояснение: Соответствия отражают назначение понятий и средств защиты. | Закрытый на сопоставление | 3 | 2 | 2 |

| *№ задания* | *Содержание задания* | *Ответ на задание* | *Тип задания* | *Время выполнения задания, мин* | *Уровень сложности (балл)* | *№ Темы* |
|---|---|---|---|---|---|---|
| | II. Подбор или утечка учетных данных<br>III. Несанкционированное чтение переписки<br>IV. Копирование конфиденциальных файлов | | | | | |
| 25. | Установите правильное соответствие между списком 1 и списком 2. Запишите буквы и соответствующие им цифры. Пример: A-II, B-I, C-IV, D-III<br><br>Установите соответствие между свойством протокола и его назначением.<br>Список 1:<br>A) Конфиденциальность<br>B) Целостность<br>C) Аутентичность<br>D) Доступность<br>Список 2:<br>I. Подтверждение участников обмена<br>II. Защита данных от чтения посторонними<br>III. Защита данных от незаметного изменения<br>IV. Возможность использовать сервис при необходимости | Правильный ответ: A-II, B-III, C-I, D-IV<br>Пояснение: Соответствия отражают назначение понятий и средств защиты. | Закрытый на сопоставление | 3 | 2 | 3 |
| 26. | Установите правильное соответствие между списком 1 и списком 2. Запишите буквы и соответствующие им цифры. Пример: A-II, B-I, C-IV, D-III<br><br>Установите соответствие между уязвимостью протокола и способом устранения.<br>Список 1:<br>A) Передача данных открытым текстом<br>B) Нет проверки целостности<br>C) Нет проверки отправителя<br>D) Повторная отправка старого сообщения<br>Список 2:<br>I. Применить шифрование<br>II. Добавить контрольную имитовставку или подпись<br>III. Использовать аутентификацию<br>IV. Добавить временную метку или одноразовый номер | Правильный ответ: A-I, B-II, C-III, D-IV<br>Пояснение: Соответствия отражают назначение понятий и средств защиты. | Закрытый на сопоставление | 3 | 2 | 3 |

| *№ задания* | *Содержание задания* | *Ответ на задание* | *Тип задания* | *Время выполнения задания, мин* | *Уровень сложности (балл)* | *№ Темы* |
|---|---|---|---|---|---|---|
| 27. | Установите правильное соответствие между списком 1 и списком 2. Запишите буквы и соответствующие им цифры. Пример: A-II, B-I, C-IV, D-III<br><br>Установите соответствие между средством Windows и его назначением.<br>Список 1:<br>A) BitLocker<br>B) IPSec<br>C) MMC<br>D) UAC<br>Список 2:<br>I. Консоль управления оснастками<br>II. Шифрование дисков<br>III. Защита сетевого обмена на уровне IP<br>IV. Контроль повышения привилегий | Правильный ответ: A-II, B-III, C-I, D-IV<br>Пояснение: Соответствия отражают назначение понятий и средств защиты. | Закрытый на сопоставление | 3 | 2 | 4 |
| 28. | Установите правильное соответствие между списком 1 и списком 2. Запишите буквы и соответствующие им цифры. Пример: A-II, B-I, C-IV, D-III<br><br>Установите соответствие между элементом политики ИБ и его содержанием.<br>Список 1:<br>A) Цель политики<br>B) Область применения<br>C) Ответственность<br>D) Контроль выполнения<br>Список 2:<br>I. Кто обязан соблюдать документ<br>II. Какие результаты защиты должны быть достигнуты<br>III. Кто отвечает за соблюдение правил<br>IV. Как проверяется выполнение требований | Правильный ответ: A-II, B-I, C-III, D-IV<br>Пояснение: Соответствия отражают назначение понятий и средств защиты. | Закрытый на сопоставление | 3 | 2 | 5 |
| 29. | Установите правильное соответствие между списком 1 и списком 2. Запишите буквы и соответствующие им цифры. Пример: A-II, B-I, C-IV, D-III<br><br>Установите соответствие между настройкой браузера и ее значением.<br>Список 1: | Правильный ответ: A-I, B-II, C-III, D-IV<br>Пояснение: Соответствия отражают назначение понятий и средств защиты. | Закрытый на сопоставление | 3 | 2 | 6 |

| *№ задания* | *Содержание задания* | *Ответ на задание* | *Тип задания* | *Время выполнения задания, мин* | *Уровень сложности (балл)* | *№ Темы* |
|---|---|---|---|---|---|---|
| | A) Обновления<br>B) Блокировка всплывающих окон<br>C) Управление cookie<br>D) Проверка HTTPS<br>Список 2:<br>I. Снижение риска эксплуатации известных уязвимостей<br>II. Уменьшение риска навязчивых и вредоносных окон<br>III. Ограничение отслеживания и хранения данных<br>IV. Проверка защищенности соединения | | | | | |
| 30. | Установите правильное соответствие между списком 1 и списком 2. Запишите буквы и соответствующие им цифры. Пример: A-II, B-I, C-IV, D-III<br><br>Установите соответствие между угрозой в браузере и мерой защиты.<br>Список 1:<br>A) Фишинговый сайт<br>B) Вредоносное расширение<br>C) Сохраненный пароль на чужом ПК<br>D) Загрузка опасного файла<br>Список 2:<br>I. Проверять адрес сайта<br>II. Устанавливать расширения из надежных источников<br>III. Не сохранять учетные данные<br>IV. Проверять файл антивирусом | Правильный ответ: A-I, B-II, C-III, D-IV<br>Пояснение: Соответствия отражают назначение понятий и средств защиты. | Закрытый на сопоставление | 3 | 2 | 6 |
| 31. | Установите правильную последовательность действий. Запишите буквы вариантов ответа в нужной последовательности без пробелов и знаков препинания.<br><br>Расположите этапы предоставления доступа к файлу в Windows.<br>A) Проверка учетной записи пользователя<br>B) Обращение пользователя к файлу<br>C) Проверка разрешений NTFS<br>D) Разрешение или запрет доступа | Правильный ответ: BACD<br>Пояснение: Последовательность отражает логический порядок выполнения действий. | Закрытый на установление последовательности | 3 | 2 | 1 |
| 32. | Установите правильную последовательность действий. Запишите буквы вариантов ответа | Правильный ответ: BACD<br>Пояснение: Последовательность отражает | Закрытый на устано | 3 | 2 | 1 |

| *№ задания* | *Содержание задания* | *Ответ на задание* | *Тип задания* | *Время выполнения задания, мин* | *Уровень сложности (балл)* | *№ Темы* |
|---|---|---|---|---|---|---|
| | в нужной последовательности без пробелов и знаков препинания.<br><br>Расположите действия администратора при настройке прав на папку.<br>A) Выбрать пользователей или группы<br>B) Открыть свойства папки и вкладку безопасности<br>C) Назначить необходимые разрешения<br>D) Проверить доступ под нужной учетной записью | логический порядок выполнения действий. | вление послед овател ьности | | | |
| 33. | Установите правильную последовательность действий. Запишите буквы вариантов ответа в нужной последовательности без пробелов и знаков препинания.<br><br>Расположите этапы анализа риска личной информационной безопасности.<br>A) Оценить вероятность и ущерб<br>B) Определить личные информационные активы<br>C) Выявить угрозы и уязвимости<br>D) Выбрать меры обработки риска | Правильный ответ: BCAD<br>Пояснение:<br>Последовательность отражает логический порядок выполнения действий. | Закрыт ый на устано вление послед овател ьности | 3 | 2 | 2 |
| 34. | Установите правильную последовательность действий. Запишите буквы вариантов ответа в нужной последовательности без пробелов и знаков препинания.<br><br>Расположите этапы разработки плана защиты личных данных.<br>A) Определить наиболее опасные риски<br>B) Составить перечень данных<br>C) Назначить меры защиты<br>D) Проверить эффективность мер | Правильный ответ: BACD<br>Пояснение:<br>Последовательность отражает логический порядок выполнения действий. | Закрыт ый на устано вление послед овател ьности | 3 | 2 | 2 |
| 35. | Установите правильную последовательность действий. Запишите буквы вариантов ответа в нужной последовательности без пробелов и знаков препинания.<br><br>Расположите этапы анализа безопасности протокола обмена информацией.<br>A) Выявить возможные атаки<br>B) Описать схему обмена | Правильный ответ: CBAD<br>Пояснение:<br>Последовательность отражает логический порядок выполнения действий. | Закрыт ый на устано вление послед овател ьности | 3 | 2 | 3 |

| *№ задания* | *Содержание задания* | *Ответ на задание* | *Тип задания* | *Время выполнения задания, мин* | *Уровень сложности (балл)* | *№ Темы* |
|---|---|---|---|---|---|---|
| | сообщениями<br>C) Определить защищаемые данные<br>D) Предложить изменение протокола | | | | | |
| 36. | Установите правильную последовательность действий. Запишите буквы вариантов ответа в нужной последовательности без пробелов и знаков препинания.<br><br>Расположите действия при устранении уязвимости протокола.<br>A) Проверить, закрыта ли уязвимость<br>B) Определить причину уязвимости<br>C) Выбрать защитный механизм<br>D) Внести изменение в протокол | Правильный ответ: BCDA<br>Пояснение:<br>Последовательность отражает логический порядок выполнения действий. | Закрытый на установление последовательности | 3 | 2 | 3 |
| 37. | Установите правильную последовательность действий. Запишите буквы вариантов ответа в нужной последовательности без пробелов и знаков препинания.<br><br>Расположите действия при включении BitLocker для диска.<br>A) Сохранить ключ восстановления<br>B) Выбрать диск для шифрования<br>C) Запустить включение BitLocker<br>D) Дождаться завершения шифрования | Правильный ответ: BCAD<br>Пояснение:<br>Последовательность отражает логический порядок выполнения действий. | Закрытый на установление последовательности | 3 | 2 | 4 |
| 38. | Установите правильную последовательность действий. Запишите буквы вариантов ответа в нужной последовательности без пробелов и знаков препинания.<br><br>Расположите действия при настройке параметра безопасности через MMC.<br>A) Открыть нужную оснастку<br>B) Запустить консоль MMC<br>C) Изменить требуемый параметр<br>D) Сохранить или применить настройки | Правильный ответ: BACD<br>Пояснение:<br>Последовательность отражает логический порядок выполнения действий. | Закрытый на установление последовательности | 3 | 2 | 4 |
| 39. | Установите правильную последовательность действий. Запишите буквы вариантов ответа в нужной последовательности без | Правильный ответ: DBCA<br>Пояснение:<br>Последовательность отражает логический порядок | Закрытый на установление | 3 | 2 | 5 |

| *№ задания* | *Содержание задания* | *Ответ на задание* | *Тип задания* | *Время выполнения задания, мин* | *Уровень сложности (балл)* | *№ Темы* |
|---|---|---|---|---|---|---|
| | пробелов и знаков препинания.<br><br>Расположите этапы разработки политики информационной безопасности.<br>A) Согласовать и утвердить документ<br>B) Определить цели и область действия<br>C) Сформулировать правила и ответственность<br>D) Проанализировать особенности организации | выполнения действий. | последовательности | | | |
| 40. | Установите правильную последовательность действий. Запишите буквы вариантов ответа в нужной последовательности без пробелов и знаков препинания.<br><br>Расположите действия безопасной настройки браузера.<br>A) Отключить или удалить ненужные расширения<br>B) Проверить наличие обновлений<br>C) Настроить защиту от опасных сайтов<br>D) Проверить параметры сохранения паролей | Правильный ответ: BCDA<br>Пояснение: Последовательность отражает логический порядок выполнения действий. | Закрытый на установление последовательности | 3 | 2 | 6 |
| 41. | Прочитайте текст вопроса и дополните фразу.<br><br>Процесс проверки личности пользователя перед предоставлением доступа называется ***. | Правильный ответ: аутентификация<br>Пояснение: Аутентификация подтверждает личность пользователя. | Открытый на дополнение | 1 | 1 | 1 |
| 42. | Прочитайте текст вопроса и дополните фразу.<br><br>Разрешения, применяемые к файлам и папкам на дисках Windows с файловой системой NTFS, называются ***. | Правильный ответ: NTFS-разрешения<br>Пояснение: Они позволяют управлять доступом к объектам файловой системы. | Открытый на дополнение | 1 | 1 | 1 |
| 43. | Прочитайте текст вопроса и дополните фразу.<br><br>Возможность реализации угрозы, приводящей к ущербу для информации или системы, называется ***. | Правильный ответ: риск<br>Пояснение: Риск объединяет вероятность события и последствия. | Открытый на дополнение | 1 | 1 | 2 |
| 44. | Прочитайте текст вопроса и | Правильный ответ: активы | Откры | 1 | 1 | 2 |

| *№ задания* | *Содержание задания* | *Ответ на задание* | *Тип задания* | *Время выполнения задания, мин* | *Уровень сложности (балл)* | *№ Темы* |
|---|---|---|---|---|---|---|
| | дополните фразу.<br><br>Данные, устройства и учетные записи, имеющие ценность для пользователя, в анализе рисков называются ***. | Пояснение: Активы являются объектами защиты. | тый на дополнение | | | |
| 45. | Прочитайте текст вопроса и дополните фразу.<br><br>Свойство протокола, обеспечивающее защиту данных от несанкционированного чтения, называется ***. | Правильный ответ: конфиденциальность<br>Пояснение: Конфиденциальность предотвращает раскрытие информации посторонним. | Открытый на дополнение | 1 | 1 | 3 |
| 46. | Прочитайте текст вопроса и дополните фразу.<br><br>Свойство протокола, позволяющее обнаружить изменение сообщения при передаче, называется ***. | Правильный ответ: целостность<br>Пояснение: Целостность защищает данные от незаметной подмены. | Открытый на дополнение | 1 | 1 | 3 |
| 47. | Прочитайте текст вопроса и дополните фразу.<br><br>Средство Windows для шифрования дисков называется ***. | Правильный ответ: BitLocker<br>Пояснение: BitLocker применяется для защиты данных на накопителе. | Открытый на дополнение | 1 | 1 | 4 |
| 48. | Прочитайте текст вопроса и дополните фразу.<br><br>Технология Windows, контролирующая повышение прав при административных действиях, называется ***. | Правильный ответ: UAC<br>Пояснение: UAC запрашивает подтверждение действий с повышенными правами. | Открытый на дополнение | 1 | 1 | 4 |
| 49. | Прочитайте текст вопроса и дополните фразу.<br><br>Документ, устанавливающий правила защиты информации в организации, называется политика *** безопасности. | Правильный ответ: информационной<br>Пояснение: Политика ИБ формализует требования к защите информации. | Открытый на дополнение | 1 | 1 | 5 |
| 50. | Прочитайте текст вопроса и дополните фразу.<br><br>Защищенный протокол передачи данных в браузере обозначается как ***. | Правильный ответ: HTTPS<br>Пояснение: HTTPS использует шифрование соединения и проверку подлинности сайта. | Открытый на дополнение | 1 | 1 | 6 |
| 51. | Прочитайте текст вопроса и дайте развернутый ответ.<br><br>Объясните, зачем в Windows | Правильный ответ: Разрешения на файлы и папки применяются для разграничения доступа | Открытый с развернутым | 4 | 4 | 1 |

| *№ задания* | *Содержание задания* | *Ответ на задание* | *Тип задания* | *Время выполнения задания, мин* | *Уровень сложности (балл)* | *№ Темы* |
|---|---|---|---|---|---|---|
| | применяются разрешения на файлы и папки. | пользователей к данным. Они определяют, кто может читать, изменять, удалять или создавать файлы. Это снижает риск несанкционированного доступа и случайного изменения информации. | ответом | | | |
| 52. | Прочитайте текст вопроса и дайте развернутый ответ.<br><br>Кратко объясните различие между аутентификацией и авторизацией. | Правильный ответ: Аутентификация подтверждает личность пользователя, например по паролю или одноразовому коду. Авторизация определяет, какие действия разрешены этому пользователю после входа в систему. Эти процессы связаны, но выполняют разные функции. | Открытый с развернутым ответом | 4 | 4 | 1 |
| 53. | Прочитайте текст вопроса и дайте развернутый ответ.<br><br>Опишите назначение анализа рисков личной информационной безопасности. | Правильный ответ: Анализ рисков нужен для выявления угроз личным данным, учетным записям и устройствам. Он помогает оценить вероятность и возможный ущерб от инцидентов. По результатам анализа выбираются меры защиты, например резервное копирование, сложные пароли и двухфакторная аутентификация. | Открытый с развернутым ответом | 4 | 4 | 2 |
| 54. | Прочитайте текст вопроса и дайте развернутый ответ.<br><br>Почему при управлении рисками важно оценивать и вероятность, и ущерб? | Правильный ответ: Вероятность показывает, насколько часто или реально может произойти угроза. Ущерб показывает тяжесть последствий для пользователя. Совместная оценка помогает определить, какие риски требуют первоочередной обработки. | Открытый с развернутым ответом | 4 | 4 | 2 |
| 55. | Прочитайте текст вопроса и дайте развернутый ответ.<br><br>Объясните, почему передача паролей открытым текстом является уязвимостью протокола. | Правильный ответ: Если пароль передается открытым текстом, злоумышленник может перехватить его в сети. После этого он сможет получить несанкционированный доступ к системе. Для защиты | Открытый с развернутым ответом | 4 | 4 | 3 |

| *№ задания* | *Содержание задания* | *Ответ на задание* | *Тип задания* | *Время выполнения задания, мин* | *Уровень сложности (балл)* | *№ Темы* |
|---|---|---|---|---|---|---|
| | | необходимо применять шифрование канала или передавать не сам пароль, а защищенный результат проверки. | | | | |
| 56. | Прочитайте текст вопроса и дайте развернутый ответ.<br><br>Какие меры можно использовать для повышения безопасности протокола обмена информацией? | Правильный ответ: Для повышения безопасности протокола применяют шифрование, аутентификацию участников и контроль целостности сообщений. Также можно использовать временные метки или одноразовые номера для защиты от повторной отправки старых сообщений. Эти меры снижают риск перехвата и подмены данных. | Открытый с развернутым ответом | 4 | 4 | 3 |
| 57. | Прочитайте текст вопроса и дайте развернутый ответ.<br><br>Объясните назначение BitLocker в Windows. | Правильный ответ: BitLocker предназначен для шифрования дисков и защиты данных при потере или краже устройства. Даже если накопитель извлекут из компьютера, данные останутся недоступными без ключа восстановления или правильной аутентификации. Это особенно важно для ноутбуков и рабочих станций с конфиденциальной информацией. | Открытый с развернутым ответом | 4 | 4 | 4 |
| 58. | Прочитайте текст вопроса и дайте развернутый ответ.<br><br>Для чего в Windows используется UAC? | Правильный ответ: UAC применяется для контроля действий, требующих административных прав. Перед изменением важных системных параметров пользователь получает запрос на подтверждение. Это помогает ограничить запуск вредоносных или случайных действий с повышенными правами. | Открытый с развернутым ответом | 4 | 4 | 4 |
| 59. | Прочитайте текст вопроса и дайте развернутый ответ.<br><br>Объясните, зачем организации нужна политика информационной | Правильный ответ: Политика информационной безопасности устанавливает единые правила защиты данных и информационных систем. В ней закрепляются | Открытый с развернутым ответо | 4 | 4 | 5 |

| *№ задания* | *Содержание задания* | *Ответ на задание* | *Тип задания* | *Время выполнения задания, мин* | *Уровень сложности (балл)* | *№ Темы* |
|---|---|---|---|---|---|---|
| | безопасности. | обязанности сотрудников, порядок доступа, требования к паролям, хранению и передаче информации. Такой документ помогает снизить риски и упорядочить работу по защите информации. | м | | | |
| 60. | Прочитайте текст вопроса и дайте развернутый ответ.<br><br>Назовите основные правила безопасной настройки браузера. | Правильный ответ: Для безопасной работы нужно регулярно обновлять браузер, использовать защиту от опасных сайтов и проверять наличие HTTPS. Не следует устанавливать неизвестные расширения и сохранять пароли на чужих компьютерах. Также важно внимательно проверять адрес сайта перед вводом учетных данных. | Открытый с развернутым ответом | 4 | 4 | 6 |

**Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующие процесс формирования компетенций в ходе освоения образовательной программы**

**Формы текущей/промежуточной аттестации**

Текущая аттестация студентов производится на практических и лабораторных занятиях в форме устного опроса и проверка отчетов по лабораторным работам. Промежуточная аттестация студентов проводится в форме зачета с оценкой. Для подготовки к промежуточной аттестации студентам выдается список вопросов для проведения зачета.

**Перечень вопросов для промежуточной аттестации (Экзамен)**

1) Определение, свойства, виды и формы представления информации;
2) Аттестация объектов по требованиям безопасности;
3) Анализ информационных ресурсов на предприятии;
4) Организация и планирование безопасности компьютерных систем;
5) Факторы и критерии принятия решения о защите компьютерных систем;
6) Лицензирование и сертификация средств защиты информации;
7) Понятие информационной безопасности;
8) Объекты информационной безопасности Российской Федерации;
9) Государственные стандарты в области защиты информации;
10) Экономические аспекты обеспечения безопасности сложных систем;
11) Правовые и организационно-технические вопросы безопасности компьютерных систем;
12) Понятие и виды конфиденциальной информации;
13) Защита конфиденциальной информации;
14) Угрозы информационной безопасности и их классификация;
15) Структура и основные элементы модели нарушителя;
16) Объекты, цели и задачи защиты компьютерных систем;
17) Категорирование ресурсов компьютерных систем и определение требований к уровню обеспечения их безопасности;
18) Принципы защиты компьютерных систем;
19) Аудит информационной безопасности, алгоритмы и методы аудита информационной безопасности;
20) Комплексный анализ безопасности компьютерных систем на методологическом, организационно-управленческом, технологическом и техническом уровнях;
21) Стратегия управления информационными рисками на основе получения их качественных и количественных оценок;
22) Понятие и признаки компьютерных преступлений, классификация компьютерных преступлений;
23) Компьютерные вирусы и принципы их функционирования;
24) Программные антивирусные средства;
25) Проблемы обеспечения программно-технологической безопасности компьютерных систем;
26) Технологическая безопасность и жизненный цикл компьютерных систем;

27) Требования, предъявляемые к архитектуре баз данных для обеспечения безопасности функционирования компьютерных систем;
28) Средства собственной защиты информационных систем;
29) Средства активной защиты компьютерных систем;
30) Средства пассивной защиты компьютерных систем;
31) Защита памяти компьютерных систем;
32) Защита выполнения программ компьютерных систем;
33) Защиты дисков компьютерных систем;
34) Средства защиты программного обеспечения с электронными ключами;
35) Уровни инфраструктуры информационной сети, источники уязвимости информационной сети;
36) Классификация атак и типовой сценарий действий потенциальных нарушителей инфраструктуры информационной сети;
37) Защитные механизмы и средства обеспечения безопасности информационной сети;
38) Краткая характеристика протоколов сетевого взаимодействия;
39) Проблемы обеспечения безопасности сетевых ОС;
40) Критерии оценки защищенности ОС;
41) Мероприятия по настройке системы безопасности сетевых ОС;
42) Криптография и криптология;
43) Обобщенная схема криптосистемы;
44) Теоретическая, практическая и временная стойкость системы криптографической защиты;
45) Симметричные алгоритмы шифрования;
46) Алгоритм шифрования DES;
47) Методы генерации псевдослучайных чисел;
48) Асимметричные алгоритмы шифрования;
49) Стандарт шифрования RSA;
50) Электронная цифровая подпись;
51) Криптографические протоколы;
52) Информационная безопасность баз данных;
53) Защита информационных ресурсов в сетях, подключенных к Internet;
54) Технические каналы утечки информации.

**Дополнительная литература**


1) Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ (последняя редакция).
2) Закон РФ от 23.09.1992 N 3523-1 (ред. от 02.02.2006) «О правовой охране программ для электронных вычислительных машин и баз данных».
3) ГОСТ Р 54593-2011 Информационные технологии (ИТ). Свободное программное обеспечение. Общие положения.
4) Савельев А.И. Лицензирование программного обеспечения в России: Законодательство и практика. – Infotropic Media, 2012. – 432 с.
5) Борисов, А. Н. Комментарий к Федеральному закону от 4 мая 2011 г. №99-ФЗ "О лицензировании отдельных видов деятельности" (постатейный) / А.Н. Борисов. - М.: Юстицинформ, 2016. - 226 с.